

The Metropolitan Corporate Counsel

www.metrocorp-counsel.com

Volume 19, No. 10

© 2011 The Metropolitan Corporate Counsel, Inc.

October 2011

Computer Forensics Is Key For Thorough And Defensible Investigations

The Editor interviews Veeral Gosalia, Senior Managing Director, FTI Consulting.

Editor: Tell us about your professional background.

Gosalia: I am a senior managing director at FTI Consulting. I assist corporations and their outside counsel with a variety of matters, including investigations, litigations and antitrust cases, which involve the collection, analysis and production of electronically stored information. After graduating college with a computer information systems degree, I joined Deloitte & Touche and worked in the e-discovery field right out of the gate. I initially practiced structured data forensics, which means working with transactional or accounting data – interrogating and analyzing to assist forensic accountants or other experts with investigations. I later joined FTI in 2002 and began training and practicing in the field of computer forensics and e-discovery more broadly. In 2007 I was given the opportunity to work in our London office for two years. It was fascinating to do discovery and conduct investigations from the perspective of a U.S. practitioner in Europe.

Editor: Without giving away confidential client information, can you give examples of some recent forensic matters you've worked on?

Gosalia: Our practice gets involved in many IP and company trade secrets theft matters, which involve employees or groups of employees who either sell or transfer important company documents to a competitor, or resign and take that information in order to form a competing business. The documents in question range from product formulas to business models to marketing information – even client lists,

proposals and pricing information.

We are typically provided with the former employee's assigned computer, and we're asked to analyze the hard drive to identify if company documents have been transferred through mediums such as USB drives, web email accounts, or perhaps burned onto a DVD. We're also working on a lot of FCPA investigations in jurisdictions where you not only have to deploy resources from abroad to assist in the matter, but you also have to understand and operate under the local data protection and privacy rules.

Editor: What are some other common scenarios for forensics today?

Gosalia: Generally, forensics is key when you need to get more context than just what the files themselves offer. For example, you may be interested in an employee's behavior just before he or she became aware that an investigation was being conducted or just before announcing he or she was leaving the firm. You may want to examine the employee's computer's registry – the database maintained within Microsoft Windows that provides information about settings and configuration of the operating system – to determine if software was installed or external devices were connected to the computer. Evidence that data-wiping software was installed on a PC while the employee was under a preservation obligation would clearly be a red flag.

I handled a matter some time ago where I imaged a hard drive and found metadata that indicated many of the documents had a "last modified" date that was before the "created" date. How can that happen? One explanation is that the files were actually



**Veeral
Gosalia**

created on another computer and moved to the PC I was provided, which led me to believe that the custodian who presented to FTI his "only computer" actually had another computer containing some of the data we were interested in finding. By simply looking at the metadata, I was able to determine the existence of another data source to which we had no access. Had the custodian simply provided me with specific documents individually, I would have missed this context and associated implication.

Editor: How can forensics help legal teams?

Gosalia: In a number of ways. At the outset of a matter, we create a preservation and collection strategy, which helps companies and counsel initially identify within the corporation (or within the IT infrastructure that the employee has access to) where relevant data might exist that is potentially responsive to the issue. We then develop a defensible data collection plan: the process must not change any of the content during the collection; it should encapsulate the relevant data; and the process must be generally accepted within the industry, as well as meet other standards.

As part of this strategy, we might recommend creating a "physical image" – by which I mean imaging a hard drive such that you're copying every bit of data on that drive without regard to the operating system or type of documents found on the drive. By creating physical images, you not only preserve the contents of the hard drive, you also allow the computer forensic examiner to have access to areas of the hard drive not visible to the user, for example, where deleted content may reside. Computer forensic examiners can also then examine operating system files to gain the context

Please email the interviewee at veeral.gosalia@fticonsulting.com with questions about this interview.

needed in certain investigations on what the user's activities have been.

Editor: Why is forensics such an important part of investigations and discovery?

Gosalia: Forensics is an important part because often you need to go beyond just the individual files and emails and look at the wider set of data that a computer forensic examiner can analyze. For example, you may also be interested to understand what, if any, files have been recently deleted and recover them. You may also want to understand which files have been recently printed or what software is or was previously installed. Preservation can also be a tricky process, and it often needs to be defended along the way. Your ability to explain it clearly will illustrate transparency, which may be key in defending your overall investigation or approach.

Editor: What are some of the emerging trends in computer forensics?

Gosalia: The types of data we're being asked to collect and analyze are changing dramatically. A few years ago, we would image hard drives and collect data from email and file servers – what I would call somewhat static places. Today, companies are using cloud-based environments and services (such as Gmail), and we're collecting a lot of data from social media sites (such as Facebook) – where there isn't necessarily just one location or field where a document resides. There are also different sets of metadata surrounding this type of content that you don't typically find in a standalone file, so our preservation approach had to change to suit today's needs. Once the data has been collected, we also need to transform copies of the preserved data into formats that our clients can review.

Editor: What can companies do to defensibly manage these emerging trends?

Gosalia: You should have a data collection plan already in place, rather than figure it out under pressure. Get ahead before it becomes a problem. Also, be sure you have an appropriate understanding of where data exists in your organization. Given some of today's companies' reliance on cloud-based services, it's highly advisable to have a data map – or at least a list of the services you use in which email or data are stored externally.

Employees should also be made aware

that when they're storing files in one of these external service providers, they're not necessarily under the care and control of the company, and they should be cautious about how they use those technologies.

Editor: When is a full forensic investigation by a third party appropriate, and when should companies conduct their own collections?

Gosalia: A full forensic investigation by a third party is appropriate when you are concerned you will have to adequately defend the process. In addition to the advantage of independence, a third party can speak to how an investigation was conducted and address any concerns about process. Also a third party may be appropriate simply when companies don't have trained internal resources that are familiar with some of the unique issues that arise in electronic discovery. When interacting with a platform or system, you'd be surprised to discover what information is residing behind closed doors versus what information is presented to you on the front end. A trained computer forensic examiner will have an understanding of this issue and will consider it during the data collection process.

Companies should conduct their own collections when they have the appropriate protocols and resources in place internally. They may have trained practitioners who are familiar with electronic evidence handling and analysis and are comfortable with defending the process if required to do so.

Editor: What are some important considerations for legal teams in selecting forensic services?

Gosalia: It's important for legal teams to ensure they are evaluating and selecting firms based on experience with the issue their client is facing and the firm's familiarity with the technologies and IT infrastructure involved. Computer forensics is a field where the phrase "experience counts" is an understatement. It's also important to ensure the firm you select understands that computer forensics is just one aspect of the overall e-discovery or investigation lifecycle. When they develop preservation and data collection plans, they must consider if the information collected can be processed and placed into a format that counsel can properly review.

Last, it's important to be aware that certain U.S. states require that electronic evidence gathered for use in court be collected by a licensed private investigator. Clients

should ensure that if they require data to be collected in a state with such a requirement that the firm they select have the appropriate license.

Editor: Can you discuss and dispel some of the common myths associated with forensics?

Gosalia: Two common myths are that you're over collecting information when making forensic physical images and that making physical images is time consuming. Many people have the misperception that a forensic image means that they will have to go in and separately weed out what they view to be the relevant data from all of other data found on the hard drive. When you make a forensic image, you're not just getting emails, Word files, Excel files, etc. – you're also getting operating system files, application files, temporary files and other documents that you might not think from the outset are useful or even required in a production.

One thing we do at FTI to help manage the sense of "over-collection" is to filter for the business documents, email and other user-generated content from the image to boil down the content to what must be processed in a traditional document review capacity, which has the added benefit of retrieving recoverable deleted files. Also, if you later want to have access to any operating system artifacts to analyze data, such as the registry, we can always access the image that contains a snapshot of the system at the time of the imaging. It's not terribly costly to perform the actual data collection effort, and typically we will bring equipment on site to rapidly image the hard drive. Separately, if you have custodians who are in faraway places, we can look at methods to remotely image their drives as well to minimize travel costs and other burdens.

Editor: To what degree do the art and science of forensics depend on technology versus traditional detective work by a qualified professional?

Gosalia: It's definitely a blend. Certainly you must know the science behind how the operating system works and what the rules are. In the example I gave earlier, science taught me that the modified date persists in certain file types as the file goes from computer to computer, but the creation date can get changed. But a different skill set is required to uncover the story behind the situation. You have to recruit your intuition and years of experience as well as technical knowledge.